

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

- - - - -x

UNITED STATES OF AMERICA

:

SEALED  
INFORMATION

- v. -

:

S1 11 Cr. 666 (LAP)

HECTOR XAVIER MONSEGUR,

:

a/k/a "Sabu,"

:

a/k/a "Xavier DeLeon,"

:

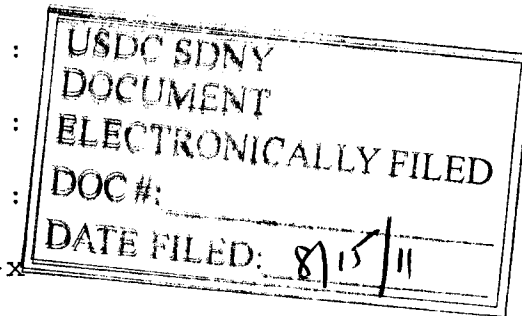
a/k/a "Leon,"

:

Defendant.

:

- - - - -x



COUNT ONE

(Conspiracy to Engage in Computer Hacking -- Anonymous)

The United States Attorney charges:

THE DEFENDANT

1. At all times relevant to this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, was an experienced computer hacker who resided in New York, New York. At various times relevant to this Information, MONSEGUR was an influential member of three hacker organizations -- Anonymous, Internet Feds, and Lulz Security (also known as "LulzSec") -- that were responsible for multiple cyber attacks on the computer systems of various businesses and governments in the United States and throughout the world.

2. At all times relevant to this Information, MONSEGUR's primary area of expertise and role in hacker

organizations was to act as a "rooter," that is, a computer hacker who identified vulnerabilities in the computer systems of potential victims to be exploited for the purpose of gaining unauthorized access to the systems. Upon discovering these vulnerabilities, MONSEGUR either passed information regarding them to other hackers, who sought to exploit them, or MONSEGUR exploited the vulnerabilities himself. MONSEGUR also provided infrastructure support to members of hacker organizations, that is, unauthorized access to computer servers and routers that others could use to launch cyber attacks on victims.

#### BACKGROUND ON ANONYMOUS

3. At all times relevant to this Information, "Anonymous" was a collective of computer hackers and other individuals located in the United States and elsewhere that undertook "operations" -- that is, coordinated efforts that included cyber attacks -- against individuals and entities that were perceived to be hostile to Anonymous and its members' interests. These attacks included, among other things, the theft and later dissemination of confidential information from computer systems and the defacement of Internet websites. These attacks also included attacks against websites, known as "denial of service" or "DoS" attacks, which involved the use of computers to bombard a victim's website with bogus requests for

information, causing the website to temporarily cease functioning.

4. The members of Anonymous, through their cyber attacks, at times sought to support, among other causes, Wikileaks, an organization that published otherwise unavailable documents from anonymous sources.

THE DEFENDANT'S COMPUTER HACKING AS PART OF ANONYMOUS

5. From in or about December 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks as part of Anonymous, including the following, among others:

DoS Attacks on Visa, MasterCard and PayPal

a. In or about December 2010, MONSEGUR briefly participated in "Operation Payback," in which members of Anonymous launched DoS attacks against the websites of the credit card companies Visa and MasterCard and the online payment service PayPal, with the intent to disrupt the operation of those companies' websites. The members of Anonymous intended Operation Payback to serve as retaliation for the refusal of Visa, MasterCard, and PayPal to process donations to Wikileaks.

Hack and DoS Attack on Tunisian Government Computers

b. In or about January 2011, MONSEGUR participated in "Operation Tunisia," in which members of

Anonymous launched cyber attacks against computer systems used by the government of Tunisia. Among other things, MONSEGUR hacked into and defaced the website of the Prime Minister of Tunisia. MONSEGUR and others also participated in a DoS attack against other websites used by the Tunisian government.

DoS Attack on Algerian Government Computers

c. In or about early 2011, MONSEGUR participated in "Operation Algeria," in which members of Anonymous launched cyber attacks against computer systems used by the government of the People's Democratic Republic of Algeria. Among other things, MONSEGUR participated in a DoS attack against websites belonging to the Algerian government.

Hack of Yemeni Government Computers

d. In or about early 2011, MONSEGUR participated in "Operation Yemen," in which members of Anonymous launched cyber attacks against computer systems used by the government of the Republic of Yemen. Among other things, MONSEGUR identified security weaknesses in these computer systems. MONSEGUR tested the security weaknesses by accessing without authorization Yemeni government computer systems and downloading certain information. MONSEGUR shared the security weaknesses with other computer hackers in Anonymous.

Hack of Zimbabwean Government Computers

e. In or about early 2011, MONSEGUR participated in "Operation Zimbabwe," in which members of Anonymous launched cyber attacks against computer systems used by the government of Zimbabwe. Among other things, MONSEGUR identified security weaknesses in those computer systems. MONSEGUR tested the security weaknesses by accessing without authorization Zimbabwean government computer systems and downloading certain information. MONSEGUR shared the security weaknesses with other computer hackers in Anonymous and attempted to steal information from a Zimbabwean government email server.

STATUTORY ALLEGATIONS

6. From at least in or about December 2010, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

7. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and

unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

OVERT ACTS

8. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about December 2010, while using a computer located in New York, New York, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in a DoS attack that was being organized by the members of Anonymous against the computer systems of PayPal, MasterCard, and Visa.

b. In or about early 2011, while using a computer located in New York, New York, MONSEGUR participated in DoS attacks against the computer systems used by the governments of Tunisia and Algeria.

c. In or about early 2011, while using a computer located in New York, New York, MONSEGUR attempted to

obtain information, without authorization, from an e-mail server used by the government of Zimbabwe.

(Title 18, United States Code, Section 1030(b).)

COUNT TWO

**(Conspiracy to Engage in Computer Hacking -- Internet Feds)**

The United States Attorney further charges:

9. The allegations in paragraphs 1 through 5 and 8 of this Information are repeated and realleged as though fully set forth herein.

BACKGROUND ON INTERNET FEDS

10. In or about December 2010, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, was invited by a co-conspirator not named as a defendant herein to participate in "Internet Feds," a group of elite computer hackers affiliated with Anonymous that undertook cyber attacks on the computer systems of various business and government entities in the United States and throughout the world. These attacks included, among other things, the theft of confidential information from victims' computer systems, the defacement of victims' Internet websites, and DoS attacks. At various times relevant to this Information, members of Internet Feds, including MONSEGUR, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others: HBGary, Inc. and HBGary

Federal, LLC (HBGary Federal, LLC is owned in part by HBGary, Inc.; both are collectively referred to herein as "HBGary"), a private cyber security firm; Fox Broadcasting Company ("Fox"), a commercial broadcast television network; and the Tribune Company, a media company which owns various television and radio stations and publishes the Chicago Tribune and the Los Angeles Times, among other newspapers. In addition, during the time period relevant to this Information, members of Internet Feds other than MONSEGUR launched computer attacks on other computer systems, including, for instance, computer servers used by ACS Law, a law firm in Australia.

THE DEFENDANT'S COMPUTER HACKING AS PART OF INTERNET FEDS

11. From in or about December 2010, up to and including in or about March 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks and unauthorized intrusions as part of Internet Feds, including the following, among others:

Hack of HBGary

a. In or about early 2011, MONSEGUR participated in a cyber attack on the computer systems of HBGary. Among other things, MONSEGUR and his co-conspirators accessed without authorization computer servers belonging to HBGary in Sacramento, California and Colorado Springs, Colorado,



and stole confidential information from those servers. In addition, MONSEGUR and his co-conspirators used information gained from this hack to, among other things, access without authorization and download emails from the email accounts of the CEO of HBGary and the owner of HBGary; access without authorization and steal confidential information from the servers for the website rootkit.com, an online forum on computer hacking maintained by the owner of HBGary; and access without authorization and deface the Twitter account of the CEO of HBGary.

Unauthorized Access to the Tribune Company's Computer Systems

b. In or about early 2011, MONSEGUR and his co-conspirators misappropriated login credentials to access the Tribune Company's computer systems without authorization.

Hack of Fox

c. In or about early 2011, MONSEGUR participated in a cyber attack on the computer systems of Fox. Among other things, MONSEGUR and his co-conspirators accessed without authorization computer servers in Los Angeles, California, belonging to Fox and stole confidential information, including information relating to contestants on "X-Factor," a Fox television show.

STATUTORY ALLEGATIONS

12. From at least in or about December 2010, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

13. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

OVERT ACTS

14. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about early 2011, while using a computer in New York, New York, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in a cyber attack on computer systems used by HBGary.

b. In our about early 2011, while using a computer in New York, New York, MONSEGUR participated in a cyber attack on computer systems used by Fox.

(Title 18, United States Code, Section 1030(b).)

### COUNT THREE

#### **(Conspiracy to Engage in Computer Hacking -- LulzSec)**

The United States Attorney further charges:

15. The allegations in paragraphs 1 through 5, 8, 10, 11 and 14 of this Information are repeated and realleged as though fully set forth herein.

### BACKGROUND ON LULZSEC

16. From in or about May 2011, up to and including in or about June 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, formed "Lulz Security," or "LulzSec," with other elite hackers, including individuals who used the online nicknames "Kayla," "Topiary," "Tflow," "Pwnsauce," and "AVUnit." "Lulz" is Internet slang which can be interpreted as "laughs," "humor," or "amusement." The members of LulzSec undertook cyber attacks on the computer

systems of various business and government entities in the United States and throughout the world. These attacks included, among other things, the theft of confidential information from victims' computer systems, the defacement of victims' Internet websites, and attacks against victims' websites which rendered the websites temporarily unavailable to the public. In addition to attacking the computer systems of their victims, the members of LulzSec also received from other computer hackers information regarding vulnerabilities in the computer security systems of a variety of business and government entities. LulzSec members used this information to launch cyber attacks on those entities or stored it in anticipation of future attacks.

17. At various times relevant to this Information, members of LulzSec launched cyber attacks on the computers systems and websites of the following victims, among others:

a. Various divisions of Sony, a global electronics and media company, including Sony Pictures Entertainment ("Sony Pictures"), which produces and distributes television shows and movies; and Sony Music Entertainment ("Sony Music"), which produces and distributes audio recordings;

b. The Public Broadcasting Service ("PBS"), a non-profit public television broadcasting service in the United States;

c. Nintendo, a video game company based in Japan;

d. The Atlanta, Georgia chapter of the Infragard Members Alliance ("Infragard-Atlanta"), an information sharing partnership between the Federal Bureau of Investigation ("FBI") and private industry concerned with protecting critical infrastructure in the United States;

e. Unveillance, a cyber security firm headquartered in Delaware;

f. The United States Senate; and

g. Bethesda Softworks, a video game company based in Maryland.

THE DEFENDANT'S COMPUTER HACKING AS PART OF LULZSEC

18. From in or about May 2011, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks as part of LulzSec, including the following, among others:

Hack of PBS

a. In or about May 2011, MONSEGUR and other members of LulzSec, in retaliation for what they perceived to be unfavorable news coverage of Wikileaks in an episode of the PBS news program Frontline, undertook a cyber attack on computer systems used by PBS. MONSEGUR and others accessed without

authorization computer servers in Alexandria, Virginia used by PBS, stole confidential information from those servers, and defaced the website for the PBS news program The News Hour, including by inserting a bogus news article that the deceased rapper Tupac Shakur was alive and living in New Zealand.

Hack of Sony Pictures

b. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR participated in a cyber attack on computer systems used by Sony Pictures. This attack included accessing without authorization and stealing confidential information from Sony Pictures' computer servers in El Segundo, California.

Hack of Sony Music

c. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR received information from another individual on a security vulnerability in Sony Music's computer systems in Belgium, the Netherlands, and Russia. MONSEGUR used that vulnerability to steal information, including the release dates of music records, from computer servers in Belgium and the Netherlands used by Sony Music. MONSEGUR also passed to other members of LulzSec the details of the security vulnerability in Sony Music's computer system in Russia.

Hacks of Infragard-Atlanta and Unveillance

d. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR and other members of LulzSec launched cyber attacks on computer systems used by Infragard-Atlanta and Unveillance. These attacks included the theft of login credentials, passwords, and other confidential information from Infragard-Atlanta and the defacement of Infragard-Atlanta's website. In addition, MONSEGUR and his co-conspirators used information gained from this hack to access without authorization, and to download, emails from the email accounts of the CEO of Unveillance.

Hack of the U.S. Senate

e. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR received from another hacker and shared with the members of LulzSec a security vulnerability in computer systems used by the United States Senate. MONSEGUR and other LulzSec members used that vulnerability to access without authorization those computer systems and to download confidential information.

Hack of Bethesda Softworks

f. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR and other members of LulzSec participated in a cyber attack on the computer

systems used by Bethesda Softworks, stealing confidential information, including usernames, passwords, and email accounts.

STATUTORY ALLEGATIONS

19. From at least in or about May 2011, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

20. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, did intentionally cause damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

OVERT ACTS

21. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among



others, were committed in the Southern District of New York and elsewhere:

a. In or about May 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by PBS that resulted in the theft of confidential information and the defacement of the website for the PBS news program The News Hour.

b. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by Sony Pictures that resulted in the theft of confidential information.

c. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by Infragard-Atlanta that resulted in the theft of confidential information from Infragard-Atlanta, which MONSEGUR and his co-conspirators used to access without authorization, and to download, emails from the email accounts of the CEO of Unveillance, and which also resulted in the defacement of Infragard-Atlanta's website.

(Title 18, United States Code, Section 1030(b).)

**COUNT FOUR**

**(Computer Hacking -- Hack of HBGary)**

The United States Attorney further charges:

22. On or about February 5, 2011, in the Eastern District of California, the Southern District of New York, and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, to wit, MONSEGUR, while using a computer located in New York, New York, together with others, accessed without authorization the computer servers of HBGary, Inc., which servers were located in Sacramento, California, and HBGary Federal, LLC, which servers were located in Colorado Springs, Colorado, and stole confidential information including email messages and other information, and thereby caused loss of at least \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A),  
1030(c)(4)(B)(i), and 2.)

**COUNT FIVE**

**(Computer Hacking -- Hack of Fox)**

The United States Attorney further charges:

23. In or about 2011, in the Central District of California, the Southern District of New York, and elsewhere,

HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, to wit, MONSEGUR, while using a computer located in New York, New York, together with others, accessed, without authorization, the servers of Fox, located in Los Angeles, California, and thereby caused loss of at least \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A),  
1030(c)(4)(B)(i), and 2.)

**COUNT SIX**

**(Computer Hacking -- Hack of Sony Pictures)**

The United States Attorney further charges:

24. In or about 2011, in the Central District of California, the Southern District of New York, and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, to wit, MONSEGUR, while using a computer located in New York, New York, together with others, accessed, without authorization, the servers of Sony Pictures,

located in El Segundo, California, and thereby caused loss of at least \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A),  
1030(c)(4)(B)(i), and 2.)

**COUNT SEVEN**

**(Computer Hacking -- Hack of PBS)**

The United States Attorney further charges:

25. From in or about May 2011, up to and including in or about June 2011, in the Eastern District of Virginia, the Southern District of New York, and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, to wit, MONSEGUR, while using a computer located in New York, New York, together with others, accessed without authorization the computer servers of PBS, which were located in Alexandria, Virginia, and stole confidential information and defaced PBS's website, PBS.org, and thereby caused loss of at least \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A),  
1030(c)(4)(B)(i), and 2.)

**COUNT EIGHT**

**(Computer Hacking -- Hack of Infragard-Atlanta)**

The United States Attorney further charges:

26. In or about June 2011, in the Northern District of Georgia, the Southern District of New York, and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, to wit, MONSEGUR, while using a computer located in New York, New York, together with others, accessed without authorization a computer server in Englewood, Colorado and elsewhere belonging to the Atlanta, Georgia chapter of the Infragard Members Alliance, an information sharing partnership between the FBI and private industry, and stole confidential information, and thereby caused loss of at least \$5,000.

(Title 18, United States Code, Sections 1030(a)(5)(A),  
1030(c)(4)(B)(i), and 2.)

**COUNT NINE**

**(Computer Hacking In Furtherance of Fraud)**

The United States Attorney further charges:

27. In or about 2010, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a

"Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly, and with intent to defraud, accessed a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained a thing of value, to wit, MONSEGUR, using a computer located in New York, New York, accessed without authorization the computer systems of a company that sells automobile parts, and fraudulently caused four automobile motors with a value of approximately \$3,450 to be shipped to himself in New York, New York.

(Title 18, United States Code, Sections 1030(a)(4),  
1030(c)(3)(A), and 2.)

**COUNT TEN**

**(Conspiracy to Commit Access Device Fraud)**

The United States Attorney further charges:

28. From at least in or about 2010, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to commit an offense under Title 18, United States Code, Section 1029(a).

29. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier

DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly, and with intent to defraud, would and did effect transactions, with one and more access devices issued to other persons, to receive payment and other things of value during a one-year period the aggregate value of which was equal to and greater than \$1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

OVERT ACTS

30. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, using a computer located in New York, New York, obtained dozens of credit card numbers of other individuals that he knew to be obtained without the authorization of the cardholders by, among other means, obtaining them from an online forum known for providing stolen credit card numbers, and by hacking into the computer systems of at least two companies.

b. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, while in New York, New York, used the credit card numbers of other individuals,

without the authorization of those individuals, to pay his own bills and, by such conduct, made and attempted to make payments in excess of \$1,000 during a one-year period.

c. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR provided, in exchange for a fee, credit card numbers of other individuals to co-conspirators not named as defendants herein, knowing that those co-conspirators planned to use the credit card numbers to make more than \$1,000 in fraudulent charges for, among other things, bills that they owed.

(Title 18, United States Code, Section 1029(b)(2).)

**COUNT ELEVEN**

**(Conspiracy to Commit Bank Fraud)**

The United States Attorney further charges:

31. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to commit offenses under Title 18, United States Code, Section 1344.

32. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and



unknown, willfully and knowingly would and did execute, and attempt to execute, a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institution by means of false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Section 1344.

OVERT ACTS

33. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, using a computer located in New York, New York, obtained the routing and account numbers for more than a dozen accounts, together with personal identification information including, among other things, names, Social Security numbers and addresses of individuals associated with those accounts.

b. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, using a computer

located in New York, New York, transmitted to a co-conspirator not named as defendants herein the aforementioned routing and account numbers, together with certain personal identification information of others, knowing that the co-conspirator would use that information to try to obtain monies to which the co-conspirator was not entitled.

(Title 18, United States Code, Section 1349.)

**COUNT TWELVE**

**(Aggravated Identity Theft)**

The United States Attorney further charges:

34. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, MONSEGUR transferred, possessed, and used, among other things, the names, Social Security numbers, account numbers, and credit card account numbers of other persons in connection with his participation in a conspiracy to commit access device fraud, as charged in Count Ten of this Information, and in connection

with his participation in a conspiracy to commit bank fraud, as charged in Count Eleven of this Information.

(Title 18, United States Code, Sections 1028A and 2.)

FORFEITURE ALLEGATION AS TO COUNTS ONE THROUGH NINE

35. As a result of committing one or more of the offenses alleged in Counts One through Nine of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of one or more of the offenses, including but not limited to a sum of money representing the amount of proceeds obtained as a result of one or more of the said offenses.

FORFEITURE ALLEGATION AS TO COUNT TEN

36. As a result of committing the offense alleged in Count Ten of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States:

a. pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, including but not limited to a sum of money representing the amount of proceeds obtained as a result of the said offense; and

b. pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the said offense.

FORFEITURE ALLEGATION AS TO COUNT ELEVEN

37. As a result of committing the offense alleged in Count Eleven of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(A), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, including but not limited to, a sum of money representing the amount of proceeds obtained as a result of the said offense.

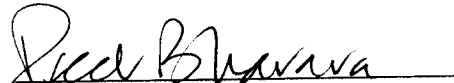
SUBSTITUTE ASSETS PROVISION

38. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
  - b. has been transferred or sold to, or deposited with, a third person;
  - c. has been placed beyond the jurisdiction of the Court;
  - d. has been substantially diminished in value;
- or

e. has been commingled with other property which cannot be subdivided without difficulty; it is the intent of the United States, pursuant to 18 U.S.C. § 982 and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982(a)(2)(A), 982(a)(2)(B), and 1029(c)(1)(C), and Title 21, United States Code, Section 853(p).)

  
PREET BHARARA  
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

---

---

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

---

---

UNITED STATES OF AMERICA

- v. -

HECTOR XAVIER MONSEGUR,  
a/k/a "Sabu,"  
a/k/a "Xavier DeLeon,"  
a/k/a "Leon,"

Defendant.

---

---

INFORMATION

S1 11 Cr. 666 (LAP)

(18 U.S.C. §§ 1030(b), 1030(a)(5)(A),  
1030(a)(4), 1029(b)(2), 1349, 1028A and 2)

---

PREET BHARARA  
United States Attorney.

---

---